PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-351747**

(43)Date of publication of application : **06.12.2002**

(51)Int.Cl. **G06F 12/16**

G06F 3/06

G06F 12/00

G06F 12/14

(21)Application number :	**2001-163202**	(71)Applicant :	**HITACHI LTD**
(22)Date of filing :	**30.05.2001**	(72)Inventor :	**SUZUKI HIROYOSHI** **TAJI IWAO**

(54) **BACKUP MANAGING METHOD FOR IN-STORAGE DATA OF STORAGE SYSTEM AND STORAGE SYSTEM EQUIPPED WITH MEANS FOR IMPLEMENTING THE SAME MANAGING METHOD**

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a backup managing method for in-storage data of a storage system which can assure high data security.

SOLUTION: The storage system includes a storage 10 having a plurality of storage areas 11 given access restrictions individually and a removable media

type backup device 30. When the data in a certain storage area 11 are backed up, the data are ciphered with a key given uniquely to the storage area 11 and the ciphered data are stored in specified removable media set in a backup device through SAN 50. When the data in the certain storage area 11 are reloaded, the removable media are set in the backup device, the ciphered data stored in the media are transmitted to the storage 10 through the SAN 50, deciphered with the key given to the storage area 11, and stored into the storage area 11.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The server equipment which accesses the storage which has two or more storage areas by which access restriction was given according to the individual, and this storage, and the backup unit of a removable media method by predetermined means of communications It is the backup management approach of the data in storage in the storage system by which network connection is carried out. By the key which gave the data of storage area A at the proper to storage area A on the occasion of backup of the data of certain storage area A of said storage areas The enciphered encryption data are stored in the predetermined removable media set in said backup unit through said communication network. The encryption data stored for setting in said backup unit on the occasion of restoration of the data of storage area A in the removable media of relevance are transmitted to said storage through said communication network. It is characterized by decrypting by said key to which this was given by storage area A, and storing in storage area A.

[Claim 2] It is the backup management approach of the data in storage in a storage system according to claim 1. Said predetermined means of communications is SAN, and said storage area is offered by one set or two or more sets of hard disk units. Encipher by the key which gave the data of a certain hard disk unit A of said hard disk units at the proper to that hard disk unit, and the storage management of this encryption data is carried out to said hard disk unit other than a hard disk unit A. Said encryption data are stored in the predetermined removable media set in said backup unit through said SAN on the occasion of backup of the data of a hard disk unit A. The removable media of relevance are set in said backup unit on the occasion of restoration of the data of a hard disk unit A. It is characterized by decrypting by said key to which the encryption data stored in this were transmitted to said storage through said SAN, and this was given by the hard disk unit A, and making it store in a hard disk unit A.

[Claim 3] It is the backup management approach of the data in storage in a storage system according to claim 2, and is characterized by setting up said access restriction by the zoning function or masking function of said SAN.

[Claim 4] It is the backup management approach of the data in storage in a storage system according to claim 2, and according to modification of the data in which said encryption data are stored by said hard disk unit A, it generates on real time, and is characterized by carrying out the storage management of said encryption data to said hard disk unit other than said hard disk unit A in concurrency.

[Claim 5] The storage system equipped with a means to enforce the backup management approach according to claim 1 to 4.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the technique for securing the data security at the time of carrying out backup management of the data in storage intensively especially using the backup unit of a removable media method about the backup management approach of the data in storage in a storage system.

[0002]

[Description of the Prior Art] The need of a data centre is growing with expansion of an ASP commercial scene, and outsourcing orientation of a company system. The outline configuration of the storage system in a typical data centre is shown in drawing 6 . The storage 10, such as disk array equipment, the server equipments 20a, 20b, and 20c which connect with the device outside a data centre through LAN, WAN, the Internet, etc., and intervene between these and storage 10, and the backup unit 30 (DAT tape drive) which backs up the data in storage 10 are connected by SAN (Storage Area Network)50.

[0003] By the way, in a data centre, in order to employ the scalable merit by package management of data in the maximum efficiently, it is common to make the data of a system which is different in one set of storage 10, or a different user intermingled, and to carry out operational administration. Therefore, in the data centre, reservation of data security is aimed at by usually giving access restriction for every system and every user computer using functions, such as zoning and masking, about each storage resource, such as a hard disk unit mounted in storage 10.

[0004] On the other hand, in the data centre, the crisis management to troubles, such as a disk crush, is also important, and the backup unit 30 connected to SAN50 using the technique of the LAN free backup and server free backup which employed the description of SAN50 efficiently is usually performing intensive backup management in the data centre. In addition, usually the operator for the thing of removable media methods, such as a comparatively cheap DAT tape drive of a bit unit price, being adopted in many cases, and performing desorption of removable media to a backup unit 30 as the aforementioned backup unit 30, is stationed.

[0005]

[Problem(s) to be Solved by the Invention] By the way, on the occasion of the desorption of the aforementioned removable media, careful cautions are required of an operator. It is because there is a possibility of the data of an alien system or a user being stored in the storage resource by which access restriction was carried out to a certain system and object for users, and leading to the serious accident in connection with trust of a data centre when the specified media and different media should be mistaken and it has set in a backup unit 30.

[0006] However, since an operator is also human being, it is difficult to prevent such an artificial mistake completely, therefore it is desirable on employment of a data centre to establish the structure which prevents such accident.

[0007] This invention is made from such a viewpoint and it aims at offering the storage system equipped with a means to enforce the backup management approach of the data in storage in a storage system that high data security is securable, and this management method.

[0008]

[Means for Solving the Problem] Main invention of this invention for attaining this purpose The server equipment which accesses the storage which has two or more storage areas by which access restriction was given according to the individual, and this storage, and the backup unit of a removable media method by predetermined means of communications It is the backup management approach of the data in storage in the storage system by which network connection is carried out. By the key which gave the data of storage area A at the proper to storage area A on the occasion of backup of the data of certain storage area A of said storage areas The enciphered encryption data are stored in the predetermined removable media set in said backup unit through said communication network. The encryption data stored for setting in said backup unit on the occasion of restoration of the data of storage area A in the removable media of relevance are transmitted to said storage through said communication network. It decrypts by said key to which this was given by storage area A, and is made to store in storage area A.

[0009]

[Embodiment of the Invention] The outline configuration of the storage system which is explained to drawing 1 as one example of this invention and which was installed in the data centre is shown. It connects with SAN50 which consisted of network devices, such as a fiber channel switch and a fiber channel bridge, and the server equipment 20 which connects with computers, such as a company which is the user of this data centre, through external networks, such as the disk array equipment 10 which functions as fiber channel storage, and WAN or the Internet, and intervenes between these and disk array equipment 10, and the DAT tape drive 30 constitute the storage system. [LAN, and]

[0010] Drawing 2 is the outline configuration of disk array equipment 10. Two or more sets of hard disk units 11 are equipped with the service processor 16 which is mounted and performs various control, a system-operating-status monitor, failure detection, various information management (for example, management of the physical number of cylinders of a hard disk unit 11, access frequency, etc. mounted) in the these-controlled drive control section 12, the channel control section 13 which controls connection between SAN50, a shared memory 14 and cache memory 15, and disk array equipment 10, etc.

[0011] Access restriction is given to the hard disk unit 11 by functions with which a fiber channel switch, disk array equipment, etc. are equipped, such as zoning and masking. For example, access restriction (zones a, b, and c) is given to hard disk units 11a, 11b, and 11c according to an individual, respectively, and hard disk units 11a, 11b, and 11c constitute the storage area which became independent, respectively, for example, in the case of drawing 1 , server equipment 20a can be accessed at hard disk unit 11a of Zone a, but neither hard disk unit 11b of Zone b nor hard disk unit 11c of Zone c can be accessed.

[0012] A part of hard disk unit 11 of disk array equipment 10 is assigned to the unit A for acting before the audience in which direct read-out and the direct writing from server equipment 20a are possible, and other parts are assigned to the unit B for shunting for storing the backup data of the unit A for acting before the audience. Matching with each unit A for acting before the audience and the unit B for shunting is set up by various kinds of approaches, such as an approach the approach which a system administrator etc. sets up manually from the administration terminal of disk array equipment 10 etc., and a service processor 16 carry out automatic recognition of the location of a slot where each hard disk unit 11 is mounted, and set it up. Disk array equipment 10 is carrying out the storage management of the matching with this unit A for acting before the audience, and the unit B for shunting to the managed table shown in drawing 3 by the unit ID of the proper to which it was given by each hard disk unit 11.

[0013] The backup data stored in the unit B for shunting encipher not the data of the unit A for acting before the audience itself but this. Disk array equipment 10 enciphers the data of each unit A for acting before the audience on real time, and stores them in real time at the unit B for shunting matched with each unit A for acting before the audience. Thereby, the storage management of the data encryption data of the unit A for acting before the audience is carried out to the unit B for shunting in concurrency.

[0014] Encryption is performed using the key set as the proper for every pair of the unit B for shunting matched with each unit A for acting before the audience, and this. A key is set up by various approaches, when are automatically generated by disk array equipment 10, and manually set up by the system administrator etc. A key is matched with the combination of the unit A for acting before the audience, and the unit B for shunting, and a storage management is carried out to said managed table.

[0015] By the way, on the occasion of backup of the data of the unit A for acting before the audience, he does not back up the data of the unit A for acting before the audience as it is, but is trying to back up the encryption data stored in the unit B for shunting matched with this in the storage system explained in this example. This is for reducing the effect on the various systems and user for whom a series of processings about backup pressed down the load given to the unit A for acting before the audience as much as possible, and use the unit A for acting before the audience.

[0016] Backup is performed by the following procedure. First, disk array equipment 10 transmits set directions of a DAT tape to the DAT tape drive 30 through SAN50. Thereby, the DAT tape drive 30 displays that a DAT tape is set to an attached administrative display. The unit ID which specifies the unit A for acting before the audience used as the candidate for backup is contained, it attaches to an administrative display at said set directions, and Unit ID is displayed on these directions here. If these displays are checked, an operator will discover the DAT tape prepared for unit A for acting before the audience of relevance from a managed rack, and will set to the DAT tape drive 30.

[0017] Next, when a DAT tape is set normally, that is notified to disk array equipment 10 through SAN50, the encryption data stored in the unit B for shunting corresponding to the unit A for acting before the audience used as the candidate for backup lead SAN50, it is transmitted to the DAT tape drive 30 from disk array equipment 10, and said encryption data are stored in said DAT tape. Completion of storing on the DAT tape of encryption data displays that on an administrative display. The operator who looked at this removes a DAT tape from the DAT tape drive 30, and contains the DAT tape in the predetermined location of an administrative rack.

[0018] On the other hand, the encryption data backed up by the DAT tape are used for restoration processing of data when the data of the unit A for acting before the audience carry out loss etc. by a disk crush etc. Below, it explains with the flow chart which shows the procedure of this restoration processing to drawing 4 .

[0019] A certain abnormalities generate disk array equipment 10 to a certain unit A for acting before the audience, and if it judges that it is necessary to use the encryption data backed up by the DAT tape, set directions of the DAT tape on which the encryption data (namely, encryption data which backed up from the unit B for shunting corresponding to this unit A for acting before the audience) corresponding to that unit A for acting before the audience are stored in the DAT tape drive 30 will be transmitted through SAN50 (110). The DAT tape drive 30 will display the unit ID of said unit A for acting before the audience accompanying the notice of this that and set demand on an administrative display, if these set directions are received (120). If these set directions are checked, an operator will discover the DAT tape of relevance from a managed rack, and will set that tape to a DAT tape drive (130).

[0020] If a DAT tape is set normally, next, that will be notified to disk array equipment 10 through SAN50, and the encryption data stored in the DAT tape set to the DAT tape drive 30 will be transmitted to disk array equipment 10. Disk array equipment 10 stores the transmitted encryption data in the unit B for shunting matched with said unit A for acting before the audience (140).

[0021] If encryption data are stored in the unit B for shunting by the above, disk array equipment 10 will try next a decryption of the encryption data memorized by the unit B for shunting by the key matched with said unit A for acting before the audience with reference to a managed table (150). In being in agreement with the key used on the occasion of the encryption data encryption by which this key is stored in the unit B for shunting here, a decryption is performed normally, disk array equipment 10 stores the decrypted data in said unit A for acting before the audience, and, thereby, data restoration processing of said unit A for acting before the audience completes it safely (160).

[0022] On the other hand, when a key is an inequality, it cannot decrypt but disk array equipment 10 displays the error message which notifies that to the display of the administration terminal of the equipment 10 concerned etc. in this case (170). and the system administrator who got to know what this was seen and a decryption was not able to carry out checks [of a DAT tape] to an operator whether the mistake has been made in whether hanging or not, and when a mistake is made in hanging, it comes out and it is, correspondence of rehaving an operator set a right DAT tape to the DAT tape drive 30 will be devised.

[0023] According to this invention, as explained above, if a key is not in agreement at all even if the encryption data of an alien system or a user are stored in the hard disk unit by which access was permitted to a certain system and user even if the operator made the mistake in hanging a DAT tape and set it, the encryption data will not be decrypted and high data security will be secured. Moreover, if a key should not be known at all even if a DAT tape is stolen, the original data cannot be restored but data security will be secured also at this point.

[0024] By the way, although the above example was the configuration of backing up the encryption data stored in the unit B for shunting For example, disk array equipment 10 enciphers the data of the unit A for acting before the audience directly. Transmit this encryption data to the DAT tape drive 30 through direct SAN50, and it backs up to removable media. At the time of data restoration, the configuration of transmitting to disk array equipment 10 and decrypting through [SAN50] the encryption data stored in the DAT tape of relevance from a DAT tape drive is also considered. In addition, when this method is adopted, as shown in drawing 1 , two or more hard disk units do not necessarily need to be contained in each zone, and one set only of a hard disk unit needs to be contained in one zone.

[0025] The method of access restriction of it not being necessarily necessary to set up access restriction per hard disk unit for example, as the above-mentioned example explained, and it dividing the storage area of one set of a hard disk unit, and giving a divided different access restriction for every storage area is also considered.

[0026] The unit A for acting before the audience and the unit B for shunting may be matched with 1:1 like the above-mentioned example, and may be matched with 1:n.

[0027] Storage may not be restricted when it is disk array equipment, but a magnetic disc system, optical-magnetic disc equipment (what was both equipped with the cache and buffer of sufficient capacity), etc. are sufficient as it.

[0028] Media, such as a cassette tape, 8mm tape, 9 truck opening tape, 3490 / 3490E cartridge, a DLT/SDLT tape, an AIT tape, a TRAVAN minicartridge tape, a DTF cartridge, a LTO cartridge, ZIP, CD-R, DVD-RAM, DVD-R, MO, and a floppy (trademark) disk, may be used for a backup unit in addition to the DAT tape drive mentioned above.

[0029] Moreover, although the hard disk unit 11 generally mounted in storage constitutes RAID in many cases, it can concern for it and apply this invention to whether RAID is constituted or not.

[0030] A key may assign the same key to the both sides of encryption and a decryption like the above-mentioned example, and may set up a cryptographic key and a decryption key separately. In addition, a cryptographic key and a decryption key will be managed by the managed table with a gestalt as shown in drawing 5 in this case.

[0031] Moreover, although premised on a private key method in the above explanation, adopting a public-key-encryption-ized method is also considered.

[0032]

[Effect of the Invention] It is possible to perform backup management of the data in storage in a storage system, securing high data security according to this invention, as explained above.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the outline configuration of the storage system installed in the data centre by one example of this invention.

[Drawing 2] It is drawing showing the outline configuration of the disk array equipment by one example of this invention.

[Drawing 3] It is drawing showing an example of the managed table by one example of this invention.

[Drawing 4] It is a flow chart explaining restoration processing of the data of the unit for acting before the audience by one example of this invention.

[Drawing 5] It is drawing showing an example of the managed table by one example of this invention.

[Drawing 6] It is drawing showing the outline configuration of the storage system in the conventional data centre.

[Description of Notations]

10 Disk Array Equipment

11 Hard Disk Unit

20a, 20b, 20c Server equipment

30 Backup Unit (DAT Tape Drive)

50 SAN